VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Absolvování individuální odborné praxe
Individual Professional Practise in the Company

2009

Filip Frank

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 7. května 2009 ….....

podpis

Poděkování

Tímto bych chtěl poděkovat vedení firmy Taurus-metal. za poskytnutí příležitosti k odborné praxi, vedení firmy za poskytnutou důvěru, všem zaměstnancům firmy za jejich spolupráci při řešení úkolů a zaměstnancům z firmy Opavský bezdrát (ISP) za pomoc a informace k VPN sítím a nasazení Linux serveru.

Abstrakt:

Tato bakalářská práce se zabývá popisem mých pracovních úkolů řešených během mé odborné praxe ve firmě Taurus-metal, kde jsem vykovával funkci správce sítě. Text se zaměřuje na popis řešení zadaných úkolů. U každého úkolu je popsán lehký úvod do problematiky a řešení tohoto úkolu. Dále je popsán souhrn praktických, ale i teoretických zkušeností a poznatků z praxe. V závěru jsou popsány dosažené výsledky v průběhu praxe a shrnutí hodnocení praxe.

Klíčová slova:

Odborná praxe, Linux, počítačové sítě, VPN, iptables, firewall, zabezpečení sítě, směrovač, Debian, SMTP

Abstract:

This bachelor work is concerned with description of my work tasks which was solved during my professional practise in Taurus-metal company where was my post of network administrator. Text is focused on description of assigned task solutions. For each task there is a short introduction to issue and its solution. Futhermore there is brief description of practical and theoretical experiences and knowledges from practise.
In conclusion there are described results which was achieved during practise and summary of practise.

Keywords:

Professional practise, Linux, computer networks, VPN, iptables, firewall, network security, router, Debian, SMTP

Seznam použitých symbolů a zkratek

VPN - Virtual private network, virtuální privátní síť
HW - Hardware, fyzické vybavení
SW - Software, programové vybavení
OS - Operating System, operační systém
NAT - Network Address Translation, překlad síťových adres
RDP - Remote Desktop Protocol, protokol pro vzdálené plochy
P2P - Peer to Peer, spojení klient-klient
ISP - Internet Service Provider, poskytovatel připojení k internetu
SMTP - Simple Mail Transfer Protocol, protokol pro přenos emailových zpráv

Obsah

1. Úvod

Nejdříve je v kapitole 2 krátce popsáno zaměření firmy a zejména zaměření mého pracovního zařazení. Přestože firma není zaměřena na IT, našla se spousta odborných úkolů, které bylo potřeba vyřešit. Dále pak následuje v kapitole 3 popis a řešení některých zadaných úkolů. Často úkoly vypadají jednoduše, ale v praxi je jejich řešení náročnější, často je nutné zvládnout a nastudovat mnohem více teorie než se na první pohled zdá. Ne vždy také zařízení, operační systémy či aplikace v praxi fungují tak, jak by měly.

Kapitola 3.1 popisuje úkol, který byl zaměřen na vyřešení problémů s hardware a software vybavením používaným ve firmě, popisuje změny ve stávajících konfiguracích a jejich důvody.

Kapitola 3.2 se zabývá vyřešením problematiky zabezpečení sítě, a vzdáleného přístupu ke službám firemní počítačové sítě.

Následující kapitola 3.3 popisuje požadavky na vytvoření informačního systému pro správu sítě, a popisuje zvolené řešení.

Poslední kapitola 3.4 se zabývá úkolem jehož cílem bylo zajistit úspěšné nasazení softwaru pro řízení výroby Exact a popisuje součásti tohoto úkolu, jehož plnění probíhalo postupně téměř celou dobu mé praxe.

Kapitola 4 obsahuje krátké shrnutí využití teoretických poznatků získaných během studia, ale i nových teoretických a praktických poznatků získaných během praxe. Je zde také sepsán seznam literatury používáné při řešení úkolů.
Na závěr je uveden souhrn dosažených výsledků a zhodnocení praxe.

2. Popis zaměření firmy a pracovního zařazení

Firma Taurus-metal se zabývá výrobou ocelového lešení a bednění. Firma je součástí skupiny Scafom International, předního evropského výrobce lešeňových systémů, s celosvětovou působností.

Mé pracovní zařazení ve firmě bylo na pozici správce sítě. Úkolem bylo postarat se kompletně o hardwarové a softwarové vybavení firmy, zlepšení kvality a spolehlivosti služeb, zvýšení zabezpečení, vyřešení problému zálohování a také vytvoření menšího informačního systému. Jedním z úkolů také bylo dokončit poslední fázi zavádění (instalace, základní zaškolení uživatelů) software Exact pro řízení výroby. Tuto práci jsem vykonával samostatně, ve firmě nebyl žádný jiný IT pracovník.

3. Zadané úkoly

3.1 Řešení problémů s používaným Software a Hardware

Prvním úkolem bylo zkontrolovat klientské počítače a to jak po stránce hardware tak i programového vybavení. Uživatelé si stěžovali na nestabilitu a pomalost svých počítačů. Zároveň bylo požadováno zkontrolovat legálnost všech používaných aplikací.

Nejdříve jsem provedl kontrolu klientských počítačů po stránce HW i SW. Některé počítače měly problémy s hardwarem, zejména způsobené vysokou teplotou, což způsobovalo nestabilitu počítačů. Často byly větrací otvory a ventilátory zaneseny prachem, v jednom případě byl ventilátor zcela zastaven. Tento problém byl odstraněn prostým vyčištěním od prachu. Dále došlo ve dvou případech k výměně základní desky z důvodu vyteklých kondenzátorů. Dále byly počítače vylepšeny tak, aby splňovaly alespoň minimální požadavky pro běh softwaru Exact, který se měl ve firmě zavádět.

Dále bylo zjištěno, že polovina počítačů nepoužívá legální operační systém. Tyto systémy nebyly ani aktualizované a to ani ty legální, na většině počítačů nebyl přítomen antivir či nástroj pro kontrolu spyware. Dalším hrubým nedostatkem bylo používání pouze Administrátorských účtů, a to všemi uživateli prakticky na všech počítačích. Na počítačích tedy bylo přítomno spousta spyware a software, který by se na pracovních stanicích vyskytovat neměl (ICQ, hry, toolbary vyhledávačů, klienti P2P a podobně).

Po dohodě s vedením byly tedy zakoupeny další licence na operační systémy, tímto však tento problém ještě vyřešen nebyl neboť nestačí pouze licence zakoupit, ale je nutné celý systém přeinstalovat. Rozhodl se vytvořit ukázkou instalaci systému, včetně programů a základního nastavení na jednom počítači a tuto instalaci poté klonovat, což by umožnilo výrazně zkrátit čas nutný k reinstalaci počítačů. Toto se povedlo jen z části, a část počítačů musela být přeinstalována běžným postupem, na vině byla především rozdílnost hardwaru počítačů s čímž se operační systémy Windows neumí vypořádat. Použitá ukázková instalace, již obsahovala všechny dostupné aktualizace operačního systému a základní aplikace. Zároveň byl systém a aplikace připraven tak, aby uživatelé nemuseli používat administrátorské účty. Byly také definovány bezpečnostní politiky operačního systému.

Konfigurace OS byla jednoduchá, nicméně se vyskytly naprosto nečekané problémy s některými aplikacemi. Nešly uživatelům spustit vůbec nebo se chovaly podivně, například si nepamatovaly změny svých nastavení, přestože pod administrátorským účtem při mém testování fungovaly bezchybně. Bylo zjištěno že některé aplikace nejsou schopny funkce pod běžným uživatelským účtem (skupina Users v OS Windows). Aplikace často zapisují své konfigurace a nastavení do svých instalačních složek, v horším případě do registrů OS Windows, kde má ovšem běžný uživatel omezená práva.

Nejjednodušší nabízené řešení v podobě povolení zápisu do všech těchto adresářů či registrů jsem ihned zavrhl. K řešení napomohly především utility z programového balíku SysinternalsSuite, internetová fóra a diskuze a také technická podpora výrobce aplikací. Takto byly identifikovány konkrétní soubory a adresáře ke kterým byl požadován přístup, následně jim byla upravena přístupová práva. Dvě úpravy se týkaly i změny práv klíčů registrů OS Windows, odhalit tyto klíče bylo obzvláště časově náročné. Postupně se takto podařilo zprovoznit všechny problémové aplikace.

3.2 Zabezpečení sítě, vytvoření vzdáleného přístupu, řešení problémů s emaily

Cílem tohoto úkolu bylo zlepšit a zajistit dostatečné zabezpečení počítačové sítě. Současně také vymyslet řešení pro bezpečné vzdálené připojení ke službám sítě, tak aby zaměstnanci mohli v případě potřeby pracovat z domova, současně mělo sloužit pro vzdálenou podporu od firmy Exact. Dále bylo požadováno vyřešit problémy s elektronickou poštou, jednak často docházelo k nespolehlivému a často pomalému odesílání zpráv, za druhé bylo potřeba vyřešit aby mohli vybraní uživatelé svou firemní poštu odesílat z různorodého internetového připojení na pracovních cestách.

Původní zabezpečení bylo dosti chabé, tvořil jej jen NAT na hlavním Zyxel směrovači od poskytovatele internetu. Sám směrovač nebyl řádně zabezpečen, rozhraní pro správu bylo otevřeno i z rozhraní internetu. S ISP tedy bylo domluveno předání tohoto routeru do naší správy, což umožnilo router nastavit dle naších potřeb, a to jak zabezpečení, tak i nutnost otevření služeb pro budoucí VPN připojení a mail server.

Dále jsem provedl rekonfiguraci Windows serveru i klientských počítačů tak, aby služby které se nepoužívají byly zakázány a nastavil bezpečnostní politiky. Bylo také vybráno antivirové řešení pro všechny počítače v síti s centrální správou. Došlo také ke změně původní struktury sítě, byly vytvořeny podsítě zvlášť pro uživatelské stanice, servery, a ostatní zařízení v síti jako je kamerový systém, převodníky RS-232-Ethernet pro docházkový systém, tiskové servery. Později při řešení VPN připojení a mail serveru, došlo k nahrazení původního hlavního routeru Linux serverem, a jako firewall bylo použito iptables. Důvody této změny budou popsány dále.

U vzdáleného připojení byla vyžadována možnost připojení k hlavnímu serveru, kde běžely důležité aplikace(účetnictví, mzdový systém, řízení výroby) a také možnost připojení ke klientským počítačům. Nejsnadnějším řešením by bylo použít takzvanou vzdálenou plochu(RDP), která je standardní součásti operačních systémů Windows(tzv. Terminálový server). Provozovat toto řešení má ale dvě zásadní nevýhody. Za prvé zabezpečení není zrovna nejlepší, RDP protokol sice nějaké šifrování samotné komunikace nabízí, nicméně k získaní

přístupu stačí pouze uhádnout přihlašovací jméno a heslo. Druhým problémem je, že nelze jednoduše zajistit rozlišení cílové stanice, neboť firma má k dispozici jen jednu veřejnou IP adresu a celá sít je tak schována za překladem adres NAT. Stanice by tak musely být rozlišeny číslem portu, což by bylo pro uživatele nepřijatelné. Navíc je takovéto přímé připojení z internetu ke klientským stanicím z hlediska bezpečnosti naprosto nevhodné.

Za vhodné řešení jsem tedy zvolil připojení k počítačové síti pomocí virtuálních privátních sítí VPN.
Uživatelé se připojí svým VPN klientem, který vytvoří dostatečně zabezpečené spojení pomocí šifrování a certifikátů, poté se jen stačilo přes tento zabezpečený kanál připojit protokolem RDP na server či svůj počítač pomocí běžného klienta vzdálené plochy a to prostým zadáním jména svého počítače.

Nejdříve byl jako server VPN zvolen stávající směrovač Zyxel, později se však po konzultaci s ISP ukázalo že router umí pouze VPN spojení dvou svých směrovačů navzájem, a tak jej nebylo možné použít pro připojování klientů.

Za technologii vhodnou pro VPN připojení jsem tedy zvolil OpenVPN, k tomuto účelu byl ze starších komponent postaven server. Jako OS byl použit Linux, jednak je zdarma ,což se zamlouvalo vedení firmy. Za druhé posloužil i jako mail server. Také jsem se chtěl o praktickém nasazení OS Linux jako serveru něco přiučit, měl jsem s ním již jisté zkušenosti, ale jen na desktopu. Distribuce byla vybrána Debian Lenny
především z důvodu stability, bezpečnosti a dostatku dokumentace. Instalace serveru a konfigurace proběhla bez větších komplikací. Vyskytly se problémy s generováním potřebných certifikátů, bylo nutné nastudovat jejich funkci, pochopit systém podepisování a také práci s balíkem openssl.

VPN připojení se poté podařilo úspěšně zprovoznit. Objevily se však občasné problémy s připojením. Tyto problémy byly způsobeny nestandardním routováním a překladem paketů na hlavním routeru, způsobené pravděpodobně vadou jeho firmware. K odhalení pomohla spolupráce s poskytovatelem internetu. Tento problém byl na doporučení odstraněn výměnou routeru Zyxel za Linux server. Ten pak sloužil jako hlavní firemní router. Bylo nutné na něm také zprovoznit služby jako je firewall, dhcp a dns server. Toto vyžadovalo získaní dalších znalostí a zkušeností, například studium funkce firewallu iptables. Odměnou však byla mnohem lepší konfigurovatelnost a větší možnosti těchto služeb, než na původním routeru. Menší problémy se ještě objevily u klientů s operačním systémem Vista, způsobené jiným systémem zabezpečení, systém neumožnil VPN klientovi vložit informace do směrovací tabulky, klient se tak tvářil jako připojen nicméně spojení nefungovalo. Tento problém byl vyřešen povolením běhu klientské aplikace pod účtem správce. Poté již s VPN připojení fungovalo bezchybně.

Další částí bylo řešení problémů s odesíláním emailů a zajištění možnosti odesílat emaily i uživatelům na pracovních cestách. Současný stav vyžadoval změnu nastavení SMTP serverů v jejich emailových klientech. Problémy s odesíláním způsobovala především občasná nestabilita připojení k internetu, s čímž měli emailoví klienti problémy. Klienti pak zbytečně obtěžovali uživatele s opakovaným odesíláním, případně výpisy chyb. Tento problém jsem se rozhodl vyřešit zprovozněním firemního emailového serveru. Bylo opět využito Linux serveru, pro službu SMTP jsem se rozhodl použít balík postfix.
Ten jsem pak sloužil jako hlavní firemní server, klienti pak odesílali své emaily na tento server, ten pak již zajistil spolehlivé doručení emailů dále. Urychlilo se tak i odesílání emailů z pohledu uživatelů, neboť po místní síti odcházely emaily mnohem rychleji, alespoň s pohledu uživatelů. K serveru byl umožněn přístup k z internetu a povoleno odesílat přes něj poštu uživatelům, kteří se ověřili svým jménem a heslem. Tak bylo zabráněno zneužití serveru pro odesílání spamu(tzv. Open-relay). Odesílání pošty z rozsahů vnitřní sítě bylo ponecháno otevřené. Uživatelé tak mohli mít nastaven pevně jeden odesílací server, bez ohledu na síť ze které se připojují.

Během provozu se objevil problém s náhodným opakovaným odesíláním zpráv. Odhalení příčin tohoto problému bylo obzvláště časově náročné, strávil jsem mnoho času různými konfiguraci SMTP serveru, problém však byl jinde. Ukázalo se že antivirový software při kontrole emailů vkládá do těla zprávy informace o nezavirovanosti zprávy. Ovšem je někdy vložil na místo kde by neměly být, což SMTP server nahlásil jako varování, přesto však zprávu odeslal dál. Antivir ale toto varování chápal jako chybu a pokoušel se zprávu odeslat znova. A tak zprávy odcházely několikrát. Problémy byl dočasně vyřešen vypnutím této antivirové kontroly, což problém vyřešilo. Zároveň byl nahlášen výrobci antiviru jako chyba. Po týdnu pak výrobce antiviru vydal opravu této chyby. Po aktualizaci antiviru již vše fungovalo bezproblémově.

3.3 Vytvoření systému pro správu sítě

Cílem toho úkolu bylo vytvořit systém pro správu a evidenci počítačů a hardware sítě, uživatelů, jejich práv a používaného software. Mělo být evidováno software nainstalované na počítačích, uživatelé kteří daný software potřebují.
Výstupem tohoto systému mělo být například:

1. Seznam přiřazení počítačů a uživatelů.
2. Výpis uživatelů kteří používají určitý software.
3. Seznam software kterému vyprší licence k zadanému datu a jejich počet.
4. Seznam počítačů a jejich IPv4 adres.
5. Seznam uživatelů kteří nemají na svém počítači nainstalován software, který potřebují pro svou práci.
6. Kontrola kolize IP adres

Tento systém jsem současně využil jako projekt v předmětu Tvorba informačních

systémů. Systém je postaven na platformě J2EE, využívá aplikačního rámce Struts 2, a nástroje Hibernate pro objektově relační mapování a usnadnění práce s databází. Tento systém tvoří webová aplikace, uživatelé k ní přistupují pomocí webového prohlížeče. Opět bylo pro nasazení této aplikace použito Linux serveru. Pro aplikaci byl využit aplikační server Apache Tomcat, a MySQL pro uložení databáze.

Systém byl po dokončení otestován a byly v něm opraveny nalezené chyby. Následně bylo provedeno předvedení systému uživatelům, kteří jej budou používat a jejich zaškolení.

3.4 Příprava a spolupráce na zavádění systému Exact

Tento úkol měl za cíl umožnit zavedení systému Exact ve firmě. Nejprve bylo nutné zajistit podmínky dodané výrobcem systému. Zejména provést úpravu hardware klientských počítačů a Windows serveru, tak aby splňovaly tyto požadavky. Dále pak s odborníky firmy Exact Software zajistit instalaci a zprovoznění systému, vyřešení zálohování, základní zaškolení uživatelů, převod stávajících dat.

Pro převod dat byl u dvou případů naprogramován jednoduchý textový konvertor dat z důvodů rozdílného formátu. Ten byl z důvodů potřeby rychlosti vývoje naprogramován v jazyce java. Dále bylo potřeba zajistit napojení ostatních aplikací k tomuto systému.

Poté bylo potřeba pomáhat řešit problémy uživatelů během zkušebního provozu. Především bylo nutné složitější problémy správně interpretovat technické podpoře, a být schopen docílit nápravy dle jejich pokynů, případně hledat problém jinde než v aplikaci.

4. Využité a získané znalosti

Během mé praxe jsem využil mnoho znalostí získaných během mého bakalářského studia, zejména z oblasti počítačových sítí, práce v počítačových sítích a správy počítačových systémů. Využil jsem však i znalosti programování a databázových systémů. Velmi užitečné byly také znalosti získané v kurzu Cisco CCNA, i když se ve firmě žádné Cisco zařízení nepoužívalo.

Málo znalostí se však projevilo především v oblasti problematiky Linuxu a služeb na něm poskytovaných. Tyto znalosti však díky dobré dokumentaci nebylo problém doplnit. Firma také byla ochotná k zakoupení dvou knih s danou problematikou.

Během praxe jsem získal zkušenosti především s operačním systémem Linux a jeho praktickým nasazením v serverovém prostředí. Užitečné také jsou zkušenosti získané s provozem serverových operačních systémů Windows, a také s praktickým provozem databází. Získal jsem také znalosti správy běžně používaných účetních, mzdových, a docházkových aplikací a systémů.

K získání chybějících znalostí při řešení úkolů byla použita především následující literatura:

Open VPN, URL: < http://openvpn.net/ >
Postfix dokumentace, URL < http://www.postfix.org/documentation.html >
Iptables, URL: < http://www.root.cz/serialy/vse-o-iptables/ >
Netfilter,iptables, URL: < http://www.netfilter.org/documentation/index.html >
Debian Linux, URL: < http://www.debian.org/doc/ >
Microsoft Developer Network, URL: < http://msdn.microsoft.com/cs-cz/default.aspx >
Microsoft technical support, URL < http://support.microsoft.com/ >
Hibernate project, URL: < http://www.hibernate.org/ >

Brůha L. *JAVA, hotová řešení.* Computer Press, 1. vyd. 2004 328s. ISBN: 80-251-0072-3
Kyle D. Dent; *Postfix - Kompletní průvodce*, Grada Publishing, 1.vyd 2005, 252 s., ISBN: 80-247-1029-3

5. Závěr

Během praxe se podařilo splnit všechny zadané úkoly a vyřešit případné problémy související s těmito úkoly. Zadávané úkoly poukazují na nutnost všeobecného rozhledu, pouhá znalost počítačových sítí zde rozhodně nestačí. Při řešení problémů existují značné rozdíly mezi školním obvykle teoretickým řešením a prostředím firemním, praktickým.

Praxe s možností řešit samostatně reálné problémy je významnou zkušeností pro budoucí povolání, případně i pro další studium.